DATA PROTECTION

THE SUPER-BRIEF GUIDE TO THE PROPOSED REGULATION

EUROPEAN DIGITAL RIGHTS

1. Definition of personal data

Why is it important?

The definition of “personal data” is key for determining the scope of the Regulation. Just because data are not linked to a name does not mean that they are not personal data. Having an appropriately wide definition of “personal data” is key to ensuring comprehensive protection of individuals. It is becoming increasingly possible to identify a person using less and less data, or to "re-identify" data previously considered anonymous.

cc by flickr.com/photos/familymwr/

What do we need?

In many cases, it is not necessary for a controller to be able to identify a specific person in order to take actions affecting his or her privacy; “singling out” a person is often enough. This should be reflected in the definition of "data subject" (i.e. the individual person) by including the aspect of “singling out”. On the other hand, a definition of “anonymous data” should be avoided, since such a definition would increase the risk of creating loopholes, if the definition was not perfect. Such flaws could then be exploited by controllers to circumvent the rules of the Regulation.

2. Consent

Why is it important?

Consent is an important legal basis for the use of personal data by the controllers (i.e. companies or public bodies). It is one of six legal grounds that can be used as a basis for the processing of personal data. Because it serves as a legal basis for processing (i.e. using) personal data, it is very important that consent be properly defined: it must mean free, deliberate and informed consent and nothing less than that.

What do we need?

Because it is an important legal basis, consent should be strong, explicit and informed under all circumstances. Also, consent must be given freely, it has to be unambiguous and must be specific. Consent should be strictly linked to the processing that the user was informed of. A user must receive sufficient information to be able to understand the consequences before he or she can give their consent to the processing and use of their data. In practice, data controllers should not be able to use "pre-ticked boxes" to gain users' consent for the processing of their personal data nor infer their consent from other actions.

3. Legitimate interest

Why is it important?

Companies and public bodies can also process personal data without consent, without the processing being necessary and without a legal obligation, if they feel that it is in their "legitimate interest" to do so - if they feel that their interests are more important than the interests of the individual "data subject" (the individual person, in other words). As a result, the legitimate interest clause creates a significant risk of being used as a "back door" by those who want to circumvent data protection rules.

What do we need?

This provision must be framed as narrowly as possible. It was originally meant to be a narrow exception and has now become the standard justification for many companies' processing of personal data. In order to reverse this trend, we need additional safeguards. The legitimate interest clause should only be allowed as a measure of last resort (namely when no other legal ground for data processing exists). It should also be justified and communicated to the public before it is used.

4. Right to be forgotten / right to erasure

Why is it important?

The right to be forgotten basically means data controllers, such as social networks, will have to comply with users' requests to delete everything they have published about themselves online. This right is very important for holding controllers accountable and empowering data subjects to have control over their own data. Supervisory authorities cannot constantly monitor all companies and public bodies, so it is crucial to give data subjects strong rights for their relationships with companies. It is important to note that this proposal does not create open-ended rights to have newspaper articles or blogs deleted or to overturn legal obligations on companies to store certain data

What do we need?

In the final Regulation, this provision should be further clarified by adding a reference to the "right to erasure". The possible exceptions for freedom of speech should be strengthened.

5. Data portability

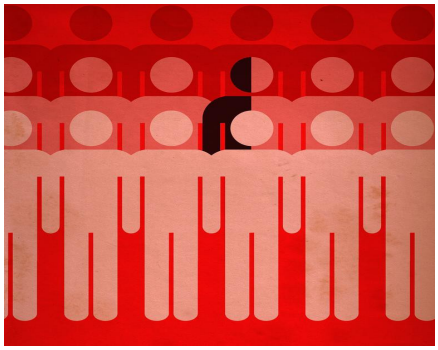
Why is it important?

This right makes it easier for users to change their service providers when they are no longer satisfied with the service they are getting. Think of a social network: you might be dissatisfied with your current provider, but by deleting your account, you would lose all the data you submitted. Data portability fixes this problem and avoids lock-in effects. This will help to stimulate competition by making market entry easier for new companies. It will also create incentives to create new services, such as to analyse your electricity use to work out if another company would be cheaper or if you could manage your usage more efficiently.

What do we need?

The right to move one's own data to another place or service should be secured as a key way of ensuring effective control over personal data. It should be clarified that the formats in which data are provided should be interoperable. Otherwise the whole excerise makes little sense because data could not easily be transferred from service to service. It should also be clarified that data controllers should not continue to store data that are no longer needed just for the purpose of being able to comply with a possible future porting request.

6. Profiling



Why is it important?

Data controllers (companies or authorities) can create profiles of citizens by collecting personal data about them. In the online environment, citizens are being 'mapped' and their profile are being evaluated, analysed and are used to predict behaviour. On the basis of their online profile, users can be provided with special offers, while other content may be withheld or prioritized differently. Governments can use profiling to guess about who may be a criminal There are 3 main problems in relation to profiling users i) profiling works on the basis that it is not perfect, but “good enough,” (especially when assessing uncommon characteristics). As a result, it can be a major problem decisions are based on an automatic process that gives a wrongful impression of this person’s behavior, health, preferences or reliability; ii) profiles can be hard or impossible to verify (which creates a risk of unreliable and discriminatory profiles that cannot be rectified) and iii) profiles are likely to perpetuate and reinforce societal inequality and discrimination against racial, ethnic, religious or other minorities.

What do we need?

The general prohibition should apply to all kinds of profiling, both online and offline. It is also essential to recognise that online identifiers are personal data, as they can “single out” individuals, even if they cannot be named. Sufficient/suitable safeguards should be put into place. For example, citizens should also have the right to be provided meaningful information about the logic behind the profiling.

7. Export to 3rd countries

Why is it important?

Most countries around the world, most particularly the USA (despite protestations to the contrary), have weaker data protection legislation and enforcement than the European Union. Weak controls on export of data means a weakening of protection of data and an incentive to process data abroad, to circumvent EU rules.

What do we need?

Data export should only be possible when verifiable guarantees are in place that the data will be processed in line with minimum EU safeguards or better.

8. Foreign law enforcement access to personal data

Why is it important?

There is a growing trend for foreign governments, particularly the USA, to claim jurisdiction on data that are held in Europe, if a company conducts systematic business in that foreign country, for example through having a registered office there. The American FISA Amendment Act, for example, permits access to "cloud computing" data for the purpose of spying on political activity of foreigners, not living in the USA. To avoid constitutional obligations, US residents are not covered by this legislation. Their free speech and privacy is protected. Ours are not.

What do we need?

Dissuasive sanctions should be in place to ensure that companies do not transfer European data outside the EU outside of agreed mutual legal assistance procedures.

9. Incompatible use

Why is it important?

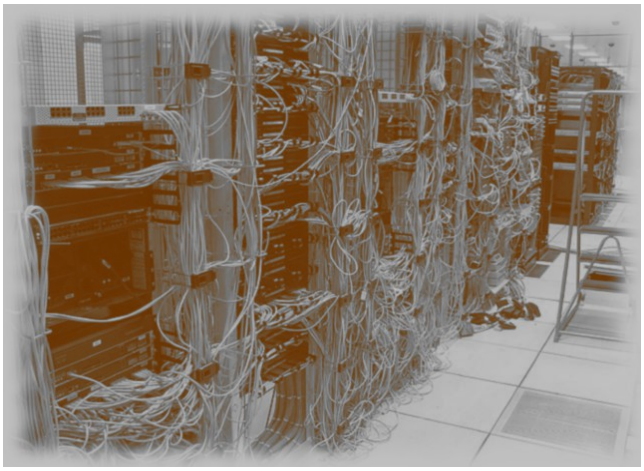
Incompatible use is the notion that you can collect data for a specific purpose, and then use it again for another, unrelated and incompatible purpose. The Commission proposed allowing this and the opinion reports by the different parliamentarians in charge of the dossier in various European Parliament committees have proposed extending it even further. This idea would completely take away the control of individuals over their data, fatally undermining the fundamental right to data protection.

What do we need?

This must be deleted. Further use of data collected for purpose A can only be re-used for another purpose on a sound legal basis and if the other purpose is compatible with the original data collection. The notion 'compatible' must be interpreted narrowly.

10. Data Protection by Design and by Default

Why is it important?



Privacy by design means that controllers of data (companies or public bodies) take a positive approach to protecting privacy, throughout the entire life cycle of technologies. Privacy by default means that when a user receives a product or service, privacy settings should be as strict as possible, without the user having to change them. By embedding privacy considerations both into the physical design of technologies and organisational practices, individuals are guaranteed a high level of protection and control over their personal data.

CC by flickr.com/photos/route79

What do we need?

This provision must be further clarified, in order to indicate that data protection by design and default relate to both (a) technical measures relating to the design and architecture of the product or service and (b) organisational measures, which relate to operational policies of the controller.

11. Strength, powers & independence of the national data protection authority

Why is it important?

Rights that cannot be enforced are worse than no rights at all. National data protection authorities are the first line of defence in protecting personal data and providing a consistent and predictable level of protection for businesses. Procedural guarantees help these authorities to maintain high standards and to foster trust.

What do we need?

In order to carry out their tasks effectively, data protection authorities must have adequate legal powers, technical expertise and financial and human resources, as well as independence from government. This independence must be firmly grounded in law.

Donate to European Digital Rights:
http://www.edri.org/about/sponsoring

http://edri.org

Rue Belliard 20
1040 Brussels